

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 21 March 2000 (21.03.00)	
International application No. PCT/EP99/04720	Applicant's or agent's file reference PAT 98502PCT
International filing date (day/month/year) 02 July 1999 (02.07.99)	Priority date (day/month/year) 03 July 1998 (03.07.98)
Applicant IMMONEN, Olli	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:

31 January 2000 (31.01.00)

☐ in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was

☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Claudio Borton
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁷ : H04L 29/06, 12/22	A1	(11) International Publication Number: WO 00/02358 (43) International Publication Date: 13 January 2000 (13.01.00)		
<table style="width: 100%; border: none;"> <tr> <td style="width: 50%; vertical-align: top; padding: 5px;"> (21) International Application Number: PCT/EP99/04720 (22) International Filing Date: 2 July 1999 (02.07.99) (30) Priority Data: PA 1998 00867 3 July 1998 (03.07.98) DK (71) Applicant (for all designated States except US): NOKIA MOBILE PHONES LIMITED [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI). (72) Inventor; and (75) Inventor/Applicant (for US only): IMMONEN, Olli [FI/FI]; Tuohuskuja 16 A 5, FIN-00670 Helsinki (FI). (74) Agents: HIGGIN, Paul et al.; Nokia House, Summit Avenue, Southwood, Farnborough, Hampshire GU14 0NG (GB). </td> <td style="width: 50%; vertical-align: top; padding: 5px;"> (81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published <i>With international search report.</i> <i>Before the expiration of the time limit for amending the</i> <i>claims and to be republished in the event of the receipt of</i> <i>amendments.</i> </td> </tr> </table>			(21) International Application Number: PCT/EP99/04720 (22) International Filing Date: 2 July 1999 (02.07.99) (30) Priority Data: PA 1998 00867 3 July 1998 (03.07.98) DK (71) Applicant (for all designated States except US): NOKIA MOBILE PHONES LIMITED [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI). (72) Inventor; and (75) Inventor/Applicant (for US only): IMMONEN, Olli [FI/FI]; Tuohuskuja 16 A 5, FIN-00670 Helsinki (FI). (74) Agents: HIGGIN, Paul et al.; Nokia House, Summit Avenue, Southwood, Farnborough, Hampshire GU14 0NG (GB).	(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published <i>With international search report.</i> <i>Before the expiration of the time limit for amending the</i> <i>claims and to be republished in the event of the receipt of</i> <i>amendments.</i>
(21) International Application Number: PCT/EP99/04720 (22) International Filing Date: 2 July 1999 (02.07.99) (30) Priority Data: PA 1998 00867 3 July 1998 (03.07.98) DK (71) Applicant (for all designated States except US): NOKIA MOBILE PHONES LIMITED [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI). (72) Inventor; and (75) Inventor/Applicant (for US only): IMMONEN, Olli [FI/FI]; Tuohuskuja 16 A 5, FIN-00670 Helsinki (FI). (74) Agents: HIGGIN, Paul et al.; Nokia House, Summit Avenue, Southwood, Farnborough, Hampshire GU14 0NG (GB).	(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published <i>With international search report.</i> <i>Before the expiration of the time limit for amending the</i> <i>claims and to be republished in the event of the receipt of</i> <i>amendments.</i>			
(54) Title: SECURE SESSION SET UP BASED ON THE WIRELESS APPLICATION PROTOCOL				
(57) Abstract <p>Method, apparatus, memory card, and system for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol. The wireless communication apparatus is provided with contact means for receiving information from a separate unit provided with memory means. The memory means comprising information to control the access of the wireless communication apparatus through a wireless communication network connected to said data communication apparatus.</p>				
<div style="display: flex; align-items: center;"> <div style="flex: 1;"> <p style="margin: 0;">Method, apparatus, memory card, and system for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol. The wireless communication apparatus is provided with contact means for receiving information from a separate unit provided with memory means. The memory means comprising information to control the access of the wireless communication apparatus through a wireless communication network connected to said data communication apparatus.</p> </div> <div style="flex: 2;"> <div style="display: flex; justify-content: space-between; margin-bottom: 10px;"> CLIENT SERVER </div> <pre> sequenceDiagram participant CLIENT participant SERVER CLIENT->>SERVER: CLIENT HELLO 100 SERVER->>CLIENT: SERVER HELLO 101 SERVER->>CLIENT: SERVER CERTIFICATE 102 SERVER->>CLIENT: SERVER KEY EXCHANGE 103 SERVER->>CLIENT: CERTIFICATE REQUEST 104 SERVER->>CLIENT: SERVER HELLO DONE 105 CLIENT->>SERVER: CLIENT CERTIFICATE 107 CLIENT->>SERVER: CLIENT KEY EXCHANGE 108 CLIENT->>SERVER: ENCRYPTED MASTER SECRET 109 SERVER->>CLIENT: CERTIFICATE VERIFY 110 CLIENT->>SERVER: FINISHED 111 SERVER->>CLIENT: FINISHED 112 CLIENT->>SERVER: DATA SESSION 113 </pre> </div> </div>				

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

Secure session set up based on the Wireless Application Protocol.

5

Technical Field of the Invention

The Wireless Application Protocol (WAP) defines an industry-wide specification for developing applications that operate over wireless communication networks. The wireless market is growing very quickly, and reaching new customers and services. To enable operators and manufacturers to meet the challenges in advanced services, differentiation and fast/flexible service creation a set of protocols has been designed in transport, security, transaction, session and application layers.

Background of the Invention

WAP security functionality includes the Wireless Transport Layer Security (WAPWTLS) and application level security, accessible using Wireless Markup Language Script (WMLScript). For optimum security, some parts of the security functionality need to be performed by a tamper-resistant device, so that an attacker cannot retrieve sensitive data. Such data is especially the permanent private keys used in WTLS handshake with client authentication, and for making application level electronic signatures (such as confirming an application level transaction). In WTLS, also master keys (master secrets) are relatively long living - which could be several days - this is in order to avoid frequent full handshakes which are quite heavy both computationally and due to relatively large data transfer. Master secrets are used as a source of entropy, to calculate MAC keys and message encryption keys which are used to secure a limited number of messages, depending on usage of WTLS.

US-A-5,307,411 describe the set up of a secure communication session between two communication units, such as phones or facsimile machines. The secure session is controlled by separate smart cards based verification units associated with a respective one of the communication units. These two
5 verification units exchanges random number, encrypts these numbers by using private keys, returns the encrypted random numbers to their origin. Then the encrypted random number is decrypted based on public keys. If the received numbers corresponds to the transmitted numbers, the parties verifies each other an the secure session may take place. However, this requires that
10 both communication units are provided with a smart card reader, which is not a necessary requirement in a server, like e.g. an Internet server. Thus, this document is quite restricting for the user, since it requires that both parties have a smart card reader, and is less suitable for communication between a wireless communication apparatus and a data communication apparatus.
15 Also, every time a session is going to be established between the two communication apparatuses, an exchange of keys must be done.

Also, US-A-5,371,794, by Sun Microsystems, discloses a way to providing a secure wireless communication link between a mobile nomadic device and a
20 base computing unit. The mobile device sends a host certificate to the base along with a randomly chosen challenge value (CH1) and a list of supported shared key algorithms. The base sends random number (RN1) encrypted in the mobile's public key and an identifier for the chosen algorithm back to the mobile. The base saves the RN1 value and adds the CH1 value and the
25 chosen algorithm to the mobile. The mobile verifies under the public key of the base the signature on the message. When the public key is verified, the mobile determines the value of RN1 by decrypting the public key under the private key of the mobile. The mobile then generates RN2 and a session key, and encrypts RN2 under the public key of the base to the base. The base
30 verifies and decrypting the RN2, and determines the session key. Finally, the

mobile and the base can enter a data transfer phase using encrypted data which is decrypted using the session key which is $RN1 + RN2$. The values of $RN1$ and $RN2$ are always derived from the last key exchange, which may be from the initial connection setup or from the last key change message, whichever is more recent. This means that each time a data transfer is made, two new numbers is generated based on $RN1$ and $RN2$, which will make the data transfer quite slow. Thus, as in US-A-5,307,411, every time a session is going to be established between the two apparatuses, in this case the mobile nomadic device and the base computing unit, an exchange of keys must be done.

Summary of the Invention

The main object of the present invention is to establish a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol.

Another object is to enable the user to re-establish a secure at a later occasion, since establishing a secure connection is a heavy procedure both computationally and due to intensive data transfer. That is why, there is a need to use the mutually agreed master secret for a relatively long time. The problem is to store the master key in a secure way. Partly due to that problem, it is common practice to restrict the lifecycle of the master secret and the associated secure session to e.g., 24 hours, after which it is required to perform the heavy key establishment procedure a new.

The main object is achieved in accordance with the present invention by connecting a wireless communication apparatus, e.g. a cellular phone, to a separate unit, e.g. a smart card, a SIM (Subscriber Identity Module) card, etc., which may store sensitive data of a secure connection. This means that the wireless communication apparatus having some kind of contact means, for

example wireless (e.g. infra-red, radio frequency, etc.) or physical (i.e. an electrical contact), for receiving information from the separate unit, i.e. the unit is provided with memory means. The memory means comprises information to control an access of the wireless communication apparatus through a
5 wireless communication network, e.g. a cellular phone network, connected to a data communication apparatus, e.g. a server, which supports a Wireless Application Protocol (WAP).

One advantage of using a separate unit, when establishing a secure
10 connection, is that it will be much easier to re-establish a connection to the data communication apparatus. Thus, it is possible to save information, e.g. signatures, secret keys, etc., in the memory means, and may be re-used in another secure connection. In order to avoid fraud, the re-use of a secure connection can be restricted for limited period of time. By saving this
15 information in the memory means the second object will be achieved.

Another advantage is that the user pays less when re-establishing a secure session, in case of the necessary information to re-establishing is saved.

20 To establish a connection, the wireless communication apparatus connects to the separate unit, accessing the wireless communication network connected to said data communication apparatus. Then the wireless communication apparatus transmits a request to the data communication apparatus. This request comprises information of which pre-defined algorithm(s) the wireless
25 communication apparatus supports. When the data communication apparatus receives this request, it chooses at least one algorithm, associated with a public key and a private key, and transmits a message back to the wireless communication apparatus. This message comprises the public key and information about which algorithm the data communication apparatus has
30 chosen. When the wireless communication apparatus receives the message,

comprising the public key, it will generate a master secret code, and calculates a signature based on the chosen algorithm, the public key and the master secret code. Thereafter, the wireless communication apparatus will transmit a respond to the data communication apparatus. This respond
5 comprises the calculated signature. When the data communication apparatus receives the respond, comprising the signature, it will calculate the master secret code based on the chosen algorithm, the signature received, and the private key. Finally, the data communication apparatus will be able to establish a secure connection to the wireless communication apparatus.

10

Further advantages of the vane arrangement according to the present invention will be apparent from the dependent claims.

15

Brief Description of the Drawing

Fig. 1 schematically illustrates a preferred embodiment of a hand portable phone according to the invention.

20

Fig. 2 schematically shows the essential parts of a telephone for communication with a cellular or cordless network.

Fig. 3 schematically shows how the secure session is set up between a client
25 /phone and a server according to the invention.

Fig. 4 illustrates the message structure for setting up a secure connection according to the invention.

Detailed Description of Embodiments

30

Fig. 1 shows a preferred embodiment of a phone according to the invention, and it will be seen that the phone, which is generally designated by 1, comprises a user interface having a keypad 2, a display 3, an on/off button 4, a speaker 5, and a microphone 6. The phone 1 according to the preferred embodiment is adapted for communication via a cellular network, but could have been designed for a cordless network as well. The keypad 2 has a first group 7 of keys as alphanumeric keys, by means of which the user can enter a telephone number, write a text message (SMS), write a name (associated with the phone number), etc. Each of the twelve alphanumeric keys 7 is provided with a figure "0-9" or a sign "#" or "*", respectively. In alpha mode each key is associated with a number of letters and special signs used in text editing.

The keypad 2 additionally comprises two soft keys 8, two call handling keys 9, and a navigation key 10.

The two soft keys 8 have a functionality corresponding to what is known from the phones Nokia 2110™, Nokia 8110™ and Nokia 3810™. The functionality of the soft key depends on the state of the phone and the navigation in the menu by using a navigation key. The present functionality of the soft keys 8 is shown in separate fields in the display 3 just above the keys 8.

The two call handling keys 9 according to the preferred embodiment are used for establishing a call or a conference call, terminating a call or rejecting an incoming call.

The navigation key 10 is an up/down key and is placed centrally on the front surface of the phone between the display 3 and the group of alphanumeric keys 7. Hereby the user will be able to control this key with his thumb. This is the best site to place an input key requiring precise motor movements. Many

experienced phone users are used to one-hand handling. They place the phone in the hand between the finger tips and the palm of the hand. Hereby the thumb is free for inputting information.

5 Fig. 2 schematically shows the most important parts of a preferred embodiment of the phone, said parts being essential to the understanding of the invention. The preferred embodiment of the phone of the invention is adapted for use in connection with the GSM network, but, of course, the invention may also be applied in connection with other phone networks, such
10 as cellular networks and various forms of cordless phone systems or in dual band phones accessing sets of these systems/networks. The microphone 6 records the user's speech, and the analog signals formed thereby are A/D converted in an A/D converter (not shown) before the speech is encoded in an audio part 14. The encoded speech signal is transferred to the controller
15 18, which i.a. supports the GSM terminal software. The controller 18 also forms the interface to the peripheral units of the apparatus, including a RAM memory 17a and a Flash ROM memory 17b, a SIM card 16, the display 3 and the keypad 2 (as well as data, power supply, etc.). The controller 18 communicates with the transmitter/receiver circuit 19. The audio part 14
20 speech-decodes the signal, which is transferred from the controller 18 to the earpiece 5 via an D/A converter (not shown).

The controller 18 is connected to the user interface. Thus, it is the controller 18 which monitors the activity in the phone and controls the display 3 in
25 response thereto.

Therefore, it is the controller 18 which detects the occurrence of a state change event and changes the state of the phone and thus the display text. A state change event may be caused by the user when he activates the keypad
30 including the navigation key 10, and this type of events is called entry events

or user events. However, the network communicating with the phone may also cause a state change event. This type of event and other events beyond the user's control are called non user events. Non user events comprise status change during call set-up, change in battery voltage, change in
5 antenna conditions, message on reception of SMS, etc.

An example of a tamper-resistant device is a smart card (SC). In the phone, it can be the Subscriber Identity Module (SIM) or an external smart card.

10 The way which a phone and a smart card interact is specified as a command-response protocol. The goal of this protocol is to provide means for a WAP handset to utilize smart cards in performing WTLS and application level security functions. The functionality presented here is based on the requirement that sensitive data, especially keys, can be stored in the card,
15 and all operations where these key are involved can be performed in the card. Different classes of the cards are introduced in order to define how widely the functionality is implemented.

This specification is based on ISO7816 series of standards on smart cards. In
20 particular, it uses the ISO7816-8 standard (draft) [ISO7816-8]. When this functionality is applied to GSM SIM there may be a need to extend also the related GSM specifications [GSM11.11], where applicable.

According to the invention the smart card 16 is used to enhance security of
25 the implementation of the Security Layer and certain functions of the Application Layer. The smart card 16 can be used for several purposes for WTLS. The major purpose of the smart card 16 is to perform cryptographic operations during the handshake, especially when the handshake is used for client authentication. Furthermore the memory of the smart card 16 is used for
30 securing a master secret, a public key and other type of confidential material

during long-living WTLS sessions. Finally the memory of the smart card 16 is used for recording the level security of the sessions. According to the invention the WTLS support in a smart card 16 can be described with reference to the following three embodiments.

5

First embodiment.

According to this embodiment, the smart card 16 is used for storage of permanent, typically certified, private keys and for performing operations using these keys. The operations includes signing operation (e.g., ECDSA or
10 RSA) for client authentication when needed for the selected handshake scheme; key exchange operation using a fixed client key (e.g., ECDH key, in ECDH_ECDSA handshake).

The smart card 16 is not required to perform the calculation of the master
15 secret or operations using the master key. These calculations may advantageously be performed by the controller 18 of the phone. However, the smart card 16 may act as a persistent storage for WTLS secure session (and connection) data, including master secrets. In this case, master secrets would be calculated and used for key derivation in the volatile phone memory (the
20 RAM 17a) but erased from there when not needed at that moment, e.g., when the user exits from secure WAP applications. Not storing session data persistently in phone 1 may improve security, e.g., in the case of a stolen phone 1. It also brings better usability in the case of changing the smart card 16 from one phone 1 to another.

25

Additionally, for portability, the smart card 16 may store needed certificates. Storage of trusted root certificates (or public keys) has significance also from security point of view: they must not be altered - but they can be exposed without danger.

30

Note that when public key encryption based key exchange (e.g., RSA) is used according to the first embodiment of the invention, there is no advantage in doing public key encryption on the smart card 16 when the pre-master secret would anyway be returned to the phone1, for master secret calculation in the
5 controller 18.

When client authentication is not supported in WTLS, at the minimum, the smart card 16 only acts as a storage for session data. If client authentication is supported, the card would be able to perform a signing operation based on
10 a private key (e.g., ECDSA or RSA) stored in the card, or key agreement calculation (e.g., ECDH) based on a fixed key stored in the card.

Second embodiment.

According to the second embodiment, the smart card 16 is used as a tamper
15 resistant device for all crypto-critical functionality: storage of all persistent keys and operations using these keys. Besides the operations performed according to the first embodiment, the smart card 16 now also supports the calculation (ECDH key exchange) or generation (RSA key exchange) of the pre-master secret; calculation and storage of the master secret for each
20 secure session; and derivation and output of key material (for MAC, encryption keys, IV, finished check), based on the master secret

The phone 1 stores MAC and message encryption keys as long as they are currently needed. These keys have a limited lifetime which may be negotiated
25 during the WTLS handshake - in the extreme case they are used for a single message only. The phone 1 has to delete the from its RAM memory 17a when the user exits from the secure WAP applications. These keys can always be derived anew from the master secret if needed.

An attacker who obtains a message encryption key can read as many messages as is agreed in the key refresh configuration (in the extreme case, a single message). An attacker who obtains a MAC key can impersonate the compromised party during as many messages as is agreed in the configuration (in the extreme case, a single message).

Third embodiment.

Certain specialized smart cards 16 may act as full-blown security engines for WTLS. This requires that the smart card 16 is equipped with its own processing unit and only uses the phone 1 as an interface to the cellular network during the secure session set up or the handshake procedure. Besides the operations according to the second embodiment, the smart card 16 may store MAC and encryption keys for each secure connection; and perform MAC calculation/verification and encryption/decryption of messages.

Furthermore the smart card 16 may be responsible for the verification of certificates and the verification of digital signatures.

Note that having message encryption in the smart card 16 does not necessarily bring any additional security because in any case the data is as plain text in the phone 1. The same is true for MAC calculation: the phone 1 must be trusted to input and output data in a correct way. The only advantage here would be not having to take encryption keys out of the card 16. However, the keys have a limited lifetime which is negotiated during the WTLS handshake - in the extreme case they are used for single message only. According to the third embodiment, the smart card 16 will contain all algorithms so that they could be controlled by smart card issuers.

Smartcard.

The term "smartcard" covers a card-like unit having some memory means in which some secret information identifying the card holder is stored. The memory means may be a magnet strip that may be read by a magnet reader, or it may be provided as discrete memory components as a ROM, EEPROM etc. When the user inserts the smart card in a more or less public apparatus he may become authorized to perform some operations such as banking operations. Presently the user of a GSM phone is identified by a so-called Subscriber Identity Module or a SIM card 16, and the structure of this type of smart card is defined in the GSM specification "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface", GSM 11.11 version 5.5.0, published by European Telecommunications Standards Institute; ETSI. The present type of smartcards will be able to support the first embodiment explained above.

15 Gemplus has recently launched a smartcard, GemXpresso RAD, based on a 32-bit chip from Texas Instruments using ARM7 RISC core technology. This 32 bit RISC processor has a 32 kbyte of non volatile flash memory and 8 kbyte of ROM. When the mechanical interface of the Gemplus card is adapted to fulfill the GSM specification this type of smartcard will be able to support the second and the third embodiment.

Network.

Fig. 3 schematically shows how the secure session, i.e. a secure connection, between a data communication apparatus and a wireless communication apparatus, e.g. a cellular phone 1. Basically the WAP content and applications are specified in a set of well-known content formats based on the familiar WWW content formats. Content is transported using a set of standard communication protocols based on the WWW communication protocols. A browser in the phone 1 co-ordinates the user interface and is

30 analogous to a standard web browser.

The wireless communication apparatus 1 is a client 1 who wants to establish a secure connection to a server 20,30,40, which is the data communication apparatus 20,20,30. The client is provided in an environment, which make it possible to reach a wide variety of different wireless platforms, e.g. world wide web (WWW). The environment provided may be referred to as Wireless Application Environment (WAE). This means that the client 1 may be supported by some kind of browser, e.g. a micro-browser, to access the different services connected to the server. In order to access these services the browser may comprise following functionalities:

- Wireless Markup Language (WML) – a lightweight markup language, similar to HTML, but optimised for use in hand-held mobile terminals;
- WMLScript – a lightweight scripting language, similar to JavaScript™;
- Wireless Telephony Application (WTA, WTAI) – telephony services and programming interfaces; and
- Content Formats – a set of well-defined data formats, including images, phone book records and calendar information.

The server 20 is using a wireless application protocol, and may comprise a gateway 30 and an origin server 40. The gateway 30 is also a server, which may identify and encrypt/decrypt information between the client 1 and the origin server 40. This means that the gateway is provided with encoders and decoders (not shown). Also, the server 20 comprises different algorithms to make the encryption/decryption. The encryption/decryption itself may be performed by well-known methods, e.g. RSA, Diffie-Hellman, etc. The origin server 40 comprises different scripts to support WAP and data to be accessed by the client. This data may be all kind of information, e.g. weather reports, news, information from stock markets, etc.

In order to access the server 20, from the client 1, the server has to be connected to a wireless communication network 50, e.g. a cellular phone network. Therefore, in accordance with the present invention, the client is provided with contact means (not shown) for receiving information from a separate unit (not shown) provided with memory means. This separate unit may be a smart card, subscriber identity module (SIM), or the like. The memory means may be a random access memory (RAM), read only memory (ROM), or the like. Further, the memory means comprises information to control the access of the server 20 through the wireless communication network 50.

To establish a secure connection, the client 1 connects to the separate unit, accessing the wireless communication network 50 connected to the server 20. Then the client 1 transmits an encrypted request 60 through the gateway 30. This encrypted request 60 comprises information of which pre-defined algorithm(s) the client 1 supports. When the gateway 30 receives this encrypted request 60, it sends 70 the encrypted request to the origin server 40. The origin server 40 chooses at least one algorithm, associated with a public key and a private key, and transmits a message 80 back to the gateway 30. The gateway encrypts the message and send it 90 to the client 1. This message 90 comprises the public key and information about which algorithm the server 20 has chosen. When the client 1 receives the encrypted message 90, comprising the public key, it will generate a master secret code, and calculates a signature based on the chosen algorithm, the public key and the master secret code. Thereafter, the client 1 will transmit an encrypted respond 65 to the gateway 30. This encrypted respond 65 comprises the calculated signature. When the gateway 30 receives the encrypted respond 80, comprising the signature, it will decrypt the respond 75 and send it to the origin server 40. The origin server will calculate the master secret code based on the chosen algorithm, the signature received, and the private key. Finally,

the origin server 40 sends a final message 85 to the client through the gateway 30. If the origin server 40 has accepted the clients 1 request 60, the server will be able to establish a secure connection between the origin server 40 and the client 1, else the connection will be terminated.

5

Setting up a secure connection.

Fig. 4 illustrates the message structure for setting up a secure connection according to the invention.

- 10 The cryptographic parameters of the secure session are produced by the WTLS Handshake Protocol, which operates on top of the WTLS Record Layer. When a WTLS client and server first start communicating, they agree on a protocol version, select cryptographic algorithms, optionally authenticate each other, and use public-key encryption techniques to generate a shared
- 15 secret.

The WTLS Handshake Protocol is described Wireless Transport Layer Security Specification dated 30. April 1998 and is a part of the Wireless Application Protocol.

20

The WTLS Handshake Protocol involves the following sequence of steps. When the a WAP session has been set between the phone 1 (the client) and the server 20 (e.g. a bank), and the client (phone 1) wants to establish a secure connection he sends a client hello message 100 as his first message.

- 25 This message includes a key exchange list that contains the cryptographic key exchange algorithms supported by the client in decreasing order of preference. In addition, each entry defines the certificate or public key the client wishes to use. The server will select one or, if no acceptable choices are presented, return a handshake_failure alert and close the secure
- 30 connection.

In response to the client hello message 100 the server 20 will send a server hello message 101 when it was able to find an acceptable set of algorithms. If it cannot find such a match, it must respond with a `handshake_failure` alert.

- 5 The server hello message 101 will identify the session and set up the parameters need for the session.

The server 20 will furthermore transmit a server certificate message 102. The server certificate message 102 will always immediately follow the server hello message 101, and the purpose of this server certificate message 102 identify the cryptation algorithm selected by the server from the key exchange list included in the client hello message 100. The server certificate message 102 will include a so-called certificate carrying a public key for the selected encryption algorithm. The server certificate message 102 includes information about issuer of the certificate, the beginning and the end of the validity period, and parameters relevant or the public key. The server controls the validity period and when the granted validity period is expired the client has to renew the secure connection. The length of the validity period will typically be in the level of a week or more. The maximum number of session will also have to be defined.

A Server Key Exchange Message 103 will be send as a third message immediately after the server certificate message 102. The server key exchange message 103 is optionally and will be sent by the server 20 only when the server certificate message 102 does not contain enough data to allow the client 1 to exchange a pre-master secret. This message 103 conveys cryptographic information to allow the client to communicate the pre-master secret: either an RSA public key to encrypt a secret with, or Elliptic Curve Diffie-Hellman parameters with which the client can complete a key exchange (with the result being the pre-master secret). As additional Key

Exchange Suites are defined for WTLS which include new key exchange algorithms, the server key exchange message will be sent if and only if the certificate type associated with the key exchange algorithm does not provide enough information for the client to exchange a pre-master secret.

5

Also a forth message - a Server Certificate message 104 - is optionally. This message 104 requests a certificate from the client, if appropriate for the selected cipher suite. This message will immediately follow the Server Certificate message 102 and Server Key Exchange message 103.

10

In order to inform the client that the server has ended of the Server Hello session, it transmits a Server Hello Done message 105. After sending this message 105 the server 20 will wait for a client response. This message indicates that the server 20 has send messages to support the key exchange, and that the client 20 can proceed with its phase of the key exchange.

15

Upon receipt of the server hello done message the client should verify that the server provided a valid certificate if required and check that the server hello parameters are acceptable.

20

If the server 20 asks for an Client Certificate message 107, the client 1 has to transmit such a after receiving a Server Hello Done message 105. This message is only sent if the server 20 requests a certificate. If no suitable certificate is available, the client must send a certificate message containing no certificates. If client authentication is required by the server for the handshake to continue, it may respond with a fatal handshake_failure alert. Client certificates are sent using the Certificate structure defined previously for server certificates.

25

Now the phone 1 or the client starts to calculate a 20 byte random number to be used as a Master Secret 106 for the secure sessions. The master secret

30

106 is used to derive key material needed for Message Authentication Code (MAC) keys and data encryption keys. MAC and data encryption provide data integrity and privacy between communicating parties. A public key based key establishment is a heavy procedure both computationally and due to intensive data transfer. That is why, there is a need to use the mutually agreed master secret 106 for a relatively long time.

The processor or the controller 18 of the phone 1 calculates the master secret. A smart card, e.g. the SIM card 16, which can be regarded as a tamper resistant device, is used for storage of the sensitive data of the secure session, and performing operations using that sensitive data, so that this data never leaves the card. In practice the secure information will be transferred from the SIM card 16 to the working RAM 17a of the processor 18 but these information will be overwritten when no session is ongoing or when the phone 1 is switched off.

According to the first embodiment of the invention the controller 18 performs the operations needed for the key establishment, e.g., Diffie-Hellman calculation or RSA encryption and complementary calculations. Then the controller 18 persistently stores the resulting secret key (master secret 106) in the SIM card 16. Then the controller 18 performs the key derivation based on the master secret 106 and additional data (e.g., seed), producing key material for MAC calculation and encryption. The key derivation function is security protocol specific. It is typically based on some secure hash function, e.g., SHA-1.

Preferably the SIM card 16 is provided as a smart card having its own processor, whereby both the operations needed for performing the key establishment and the key derivation based on the master secret may be performed inside the smart card. Then the master secret, and data used to

calculate it, would never have to leave smart card. So, the secure session associated with the master secret can be used during a long period

5 A Client Key Exchange Message 108 will immediately follow the client certificate message 107, if it is sent. Otherwise it will be the first message sent by the client 1 after it receives the Server Hello Done message 105. With this message 108, a pre-master secret is set, either through direct transmission of the RSA-encrypted secret, or by the transmission of EC Diffie-Hellman public key which will allow each side to agree upon the same pre-master secret.

10

Then the Master Secret 106 is encrypted by using the public key from the server's certificate and the agreed RSA algorithm. The result is send to the server 20 in an encrypted master secret message 109.

15 A Certificate Verify message 110 is used to provide explicit verification of a client certificate. This message is only sent by the client following a client certificate Message 107 that has signing capability (i.e., RSA certificates).

Both ends has to send finished messages 111 and 112 at the end of the
20 handshake to verify that the key exchange and authentication processes were successful.

The finished messages 111 and 112 is the first messages protected with the just-negotiated algorithms, keys, and secrets. Recipients of finished
25 messages must verify that the contents are correct. Once a side has sent its Finished message and received and validated the Finished message from its peer, it may begin to send and receive application data 113 over the secure connection. It is a critical or fatal error if a finished message is not preceded by a change cipher spec message at the appropriate point in the handshake.

30

The value handshake_messages includes all handshake messages starting at client hello up to, but not including, this finished message. The handshake_messages for the finished message sent by the client will be different from that for the finished message sent by the server, because the one which is sent second will include the prior one.

As long as a secure connection is valid application data session 113 may be initiated just by using Client Hello messages 100 and Server Hello messages 101.

10

Acronyms.

	APDU	Application Protocol Data Unit
	API	Application Programming Interface
	CA	Certification Authority
15	CBC	Cipher Block Chaining
	DF	Dedicated File
	DH	Diffie-Hellman
	EC	Elliptic Curve
	ECC	Elliptic Curve Cryptography
20	ECDH	Elliptic Curve Diffie-Hellman
	ECDSA	Elliptic Curve Digital Signature Algorithm
	EF	Elementary File
	GSM	Global System for Mobile Communication
	IV	Initialization Vector
25	MAC	Message Authentication Code
	ME	Management Entity
	OSI	Open System Interconnection
	PDU	Protocol Data Unit
	PRF	Pseudo-Random Function
30	SAP	Service Access Point

	SDU	Service Data Unit
	SHA-1	Secure Hash Algorithm
	SIM	Subscriber Identity Module
	SMS	Short Message Service
5	SSL	Secure Sockets Layer
	TLS	Transport Layer Security
	WAP	Wireless Application Protocol
	WML	Wireless Markup Language
	WMLScript	Wireless Markup LanguageScript
10	WDP	Wireless Datagram Protocol
	WSP	Wireless Session Protocol
	WTLS	Wireless Transport Layer Security
	WTP	Wireless Transaction Protocol

- 15 The list above includes the acronyms used in the present text. Detailed discussion and explanation of the acronyms may be found in the technical specifications defining the Wireless Application Protocol on the Internet homepage for WAPFORUM, <http://www.wapforum.org/>.

CLAIMS

1. Method for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on
5 a wireless application protocol, wherein said wireless communication apparatus having contact means for receiving information from a separate unit provided with memory means, said memory means comprising information to control the access of the wireless communication apparatus through a wireless communication network connected to said data
10 communication apparatus, comprising the following steps:
- connecting said wireless communication apparatus to the separate unit, accessing the wireless communication network connected to said data communication apparatus
 - the wireless communication apparatus transmits a request to the data
15 communication apparatus to establish a connection, said request comprising information of which pre-defined algorithm(s) the wireless communication apparatus supports,
 - upon reception of said request, the data communication apparatus choose at least one algorithm, associated with a public key and a
20 private key, and transmits a message back to the wireless communication apparatus, said message comprising the public key and information about which algorithm the data communication apparatus has chosen,
 - upon reception of the message, comprising the public key, the wireless
25 communication apparatus generates a master secret code, and calculates a signature based on the chosen algorithm, the public key and the master secret code, and transmits a respond to the data communication apparatus, said respond comprising the calculated signature,

- upon reception of the respond comprising the signature, the data communication apparatus calculates the master secret code based on the chosen algorithm, the signature received and the private key, and establish a secure connection to the wireless communication apparatus, and
 - saving said master secret code on said memory means and in the data communication apparatus, in order to re-establish the connection at a later occasion.
- 5
- 10 2. A method according to claim 1, and comprising a step of saving said master secret under a pre-defined time.
3. A method according to claim 1 or 2, and comprising a step of re-establishing the connection by
- 15 - transmitting a request from the wireless communication apparatus to the data communication apparatus, said request comprising the calculated signature based on the chosen algorithm, the public key and the stored secret key, and
- upon reception of the request, the data communication apparatus
- 20 calculates the master secret code based on the chosen algorithm, the signature received, and the private key, and, establish a secure connection to the wireless communication apparatus.
4. A method according to claim 1, 2, or 3, and comprising a step of providing
- 25 said memory means in a smart card.
5. Wireless communication apparatus for establishing a secure connection to a data communication apparatus based on a wireless application protocol, said wireless communication apparatus comprising:

24

- communication means for establishing a connection to a wireless communication network connected to said data communication apparatus,
 - contact means for receiving information from a separate unit provided with memory means, said memory means is provided with information to control the access of the data communication apparatus through the wireless communication network,
 - reading means for reading information received from the data communication apparatus and the information provided on said memory means,
 - random generating means, for generating a master secret code,
 - pre-defined algorithm(s), to generate a signature based on said master secret code and a public key received from said data communication apparatus, which is to be used when the wireless communication apparatus is going to establish a secure connection to the data communication apparatus, and
 - said reading means comprising a secure database provided with at least one master secret code and/or at least one signature related to one or more data communication apparatus, in order to re-establish a secure connection to a data communication apparatus.
6. A wireless communication apparatus according to claim 5, having its memory means exchangeable.
7. An apparatus according to claim 5 or 6, said memory means is a smart card.
8. An apparatus according to claim 5, 6, or 7, said memory means is a subscriber identity module.

30

9. Memory card for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol, arranged to be connected to said wireless communication apparatus having contact means for receiving information from the memory card, and said memory card is provided with information to control the access of the data communication apparatus through a wireless communication network.
10. A memory card according to claim 9, further comprising encryption means for encrypting the master secret, which is to be used as a signature for the wireless communication apparatus when it is establishing a secure connection.
11. A memory card according to claim 9 or 10, comprising a secure database provided with at least one master secret code and/or at least one signature related to one or more data communication apparatus, in order to re-establish a secure connection to a data communication apparatus.
12. A memory card according to claim 9, 10, or 11, is provided on a smart card.
13. System for establishing a secure connection when using a wireless application protocol, comprising:
- a data communication apparatus based on the wireless application protocol,
 - a wireless communication network, connected to said data communication apparatus,
 - a wireless communication apparatus having contact means for receiving information from a separate unit provided with memory means, and

- the separate unit provided with the memory means, said memory means, comprising information to control the access of the wireless communication apparatus through the wireless communication network, wherein
- 5 - the wireless communication apparatus is arranged to transmit a request to the data communication apparatus to establish a connection, said request comprising information of which pre-defined algorithm(s) the wireless communication apparatus supports,
- 10 - upon reception of said request, the data communication apparatus is arranged to choose at least one algorithm, associated with a public key and a private key, and to transmit a message back to the wireless communication apparatus, said message comprising the public key and information about which algorithm the data communication apparatus will choose,
- 15 - upon reception of said message, comprising the public key, the wireless communication apparatus is arranged to generate a master secret code, to calculate a signature based on the chosen algorithm, the public key and the master secret code, and to transmit a respond to the data communication apparatus, said respond comprising the
- 20 calculated signature,
- upon reception of the respond comprising the signature, the data communication apparatus is arranged to calculate the master secret code based on the chosen algorithm, the signature received, and the private key, and, thus establish a secure connection to the wireless
- 25 communication apparatus, and
- said memory means and the data communication apparatus are arranged to save said master secret code, in order to re-establish the connection at a later occasion.

27

14. A system according to claim 13, said master secret is arranged to be saved under a pre-defined time.

15. A system according to claim 13, or 14, said memory means is a smart
5 card.

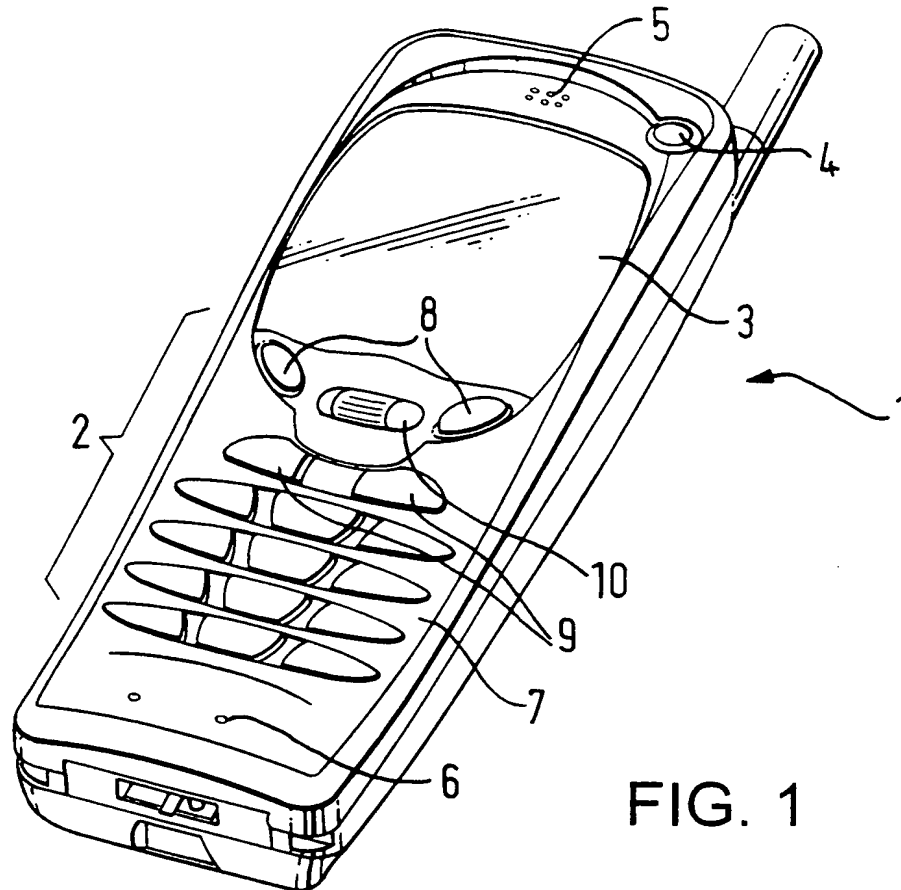


FIG. 1

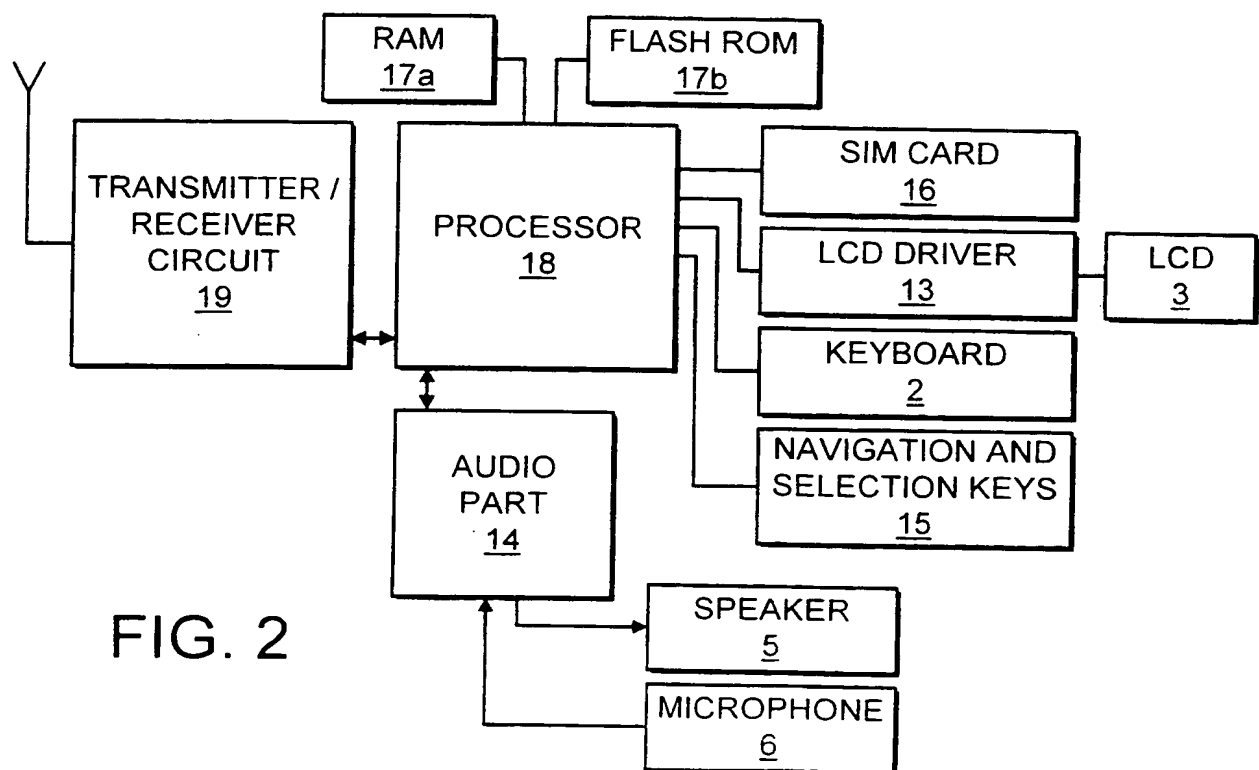


FIG. 2

2 / 2

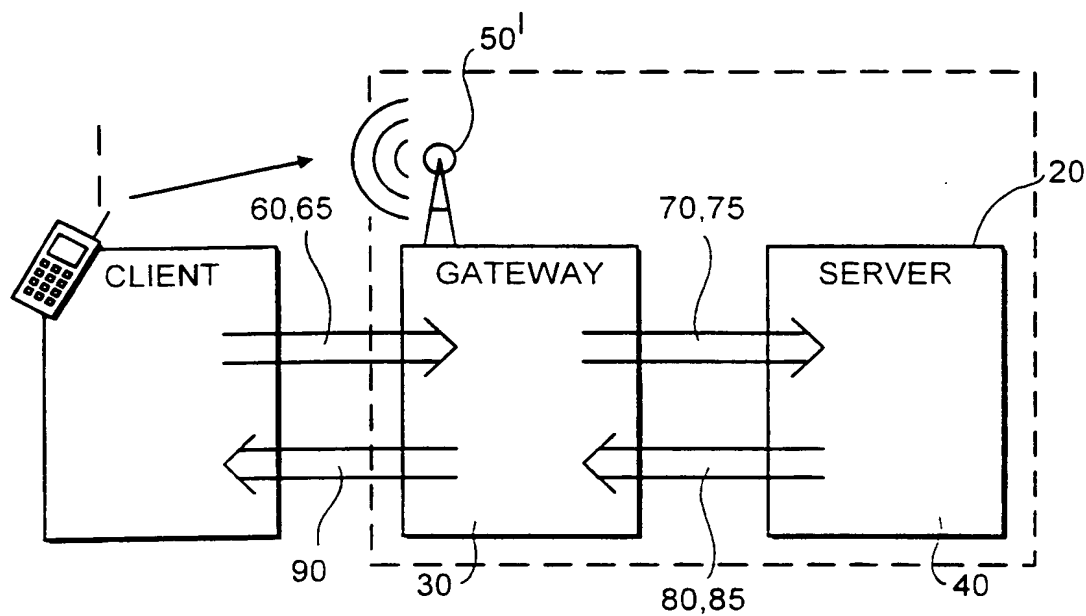


FIG. 3

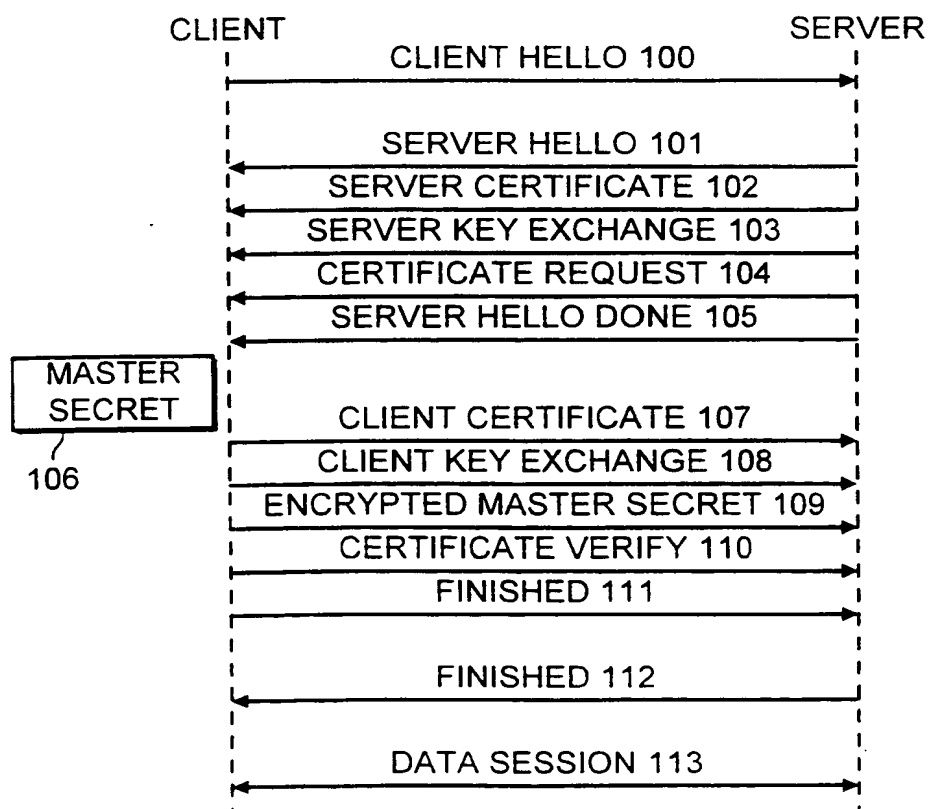


FIG. 4

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference PAT 98502PCT	FOR FURTHER ACTION see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/EP 99/ 04720	International filing date (day/month/year) 02/07/1999	(Earliest) Priority Date (day/month/year) 03/07/1998
Applicant NOKIA MOBILE PHONES LIMITED et al.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.
☒ It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

- a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

- b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. ☐ **Certain claims were found unsearchable** (See Box I).

3. ☐ **Unity of invention is lacking** (see Box II).

4. With regard to the **title**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No.

☒ as suggested by the applicant.

☐ because the applicant failed to suggest a figure.

☐ because this figure better characterizes the invention.

4

☐ None of the figures.

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 99/04720

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L29/06 H04L12/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A ✓	DE 195 42 732 A (SCHEINERT STEFAN) 22 May 1997 (1997-05-22) abstract column 1, line 21 -column 3, line 1 column 3, line 45-57 ---	1-15
A ✓	EP 0 538 216 A (TELEVERKET) 21 April 1993 (1993-04-21) cited in the application abstract column 1, line 29-40 column 2, line 5-30 column 3, line 28-52 column 5, line 8-27 ---	1-15
	--- -/--	



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

° Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

19 November 1999

Date of mailing of the international search report

03/12/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Lázaro López, M.L.

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 99/04720

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>SIEMENS: "Banking by Mobile Phone" TELCOMREPORT, 30 June 1998 (1998-06-30), XP002123311 Available from Internet <http://www.siemens.de/telcom/articles/e0198/198habak.html> 30 June 1998 the whole document -----</p>	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 99/04720

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
DE 19542732	A	22-05-1997	NONE	
EP 0538216	A	21-04-1993	SE 470001 B	18-10-1993
			DE 69218335 D	24-04-1997
			DE 69218335 T	09-10-1997
			ES 2099243 T	16-05-1997
			JP 6125342 A	06-05-1994
			SE 9102641 A	13-03-1993
			US 5307411 A	26-04-1994

REPLACED BY
PCT/EP/409

PATENT COOPERATION TREATY

PCT

REC'D 16 OCT 2000

WIPO PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

15

Applicant's or agent's file reference PAT 98502PCT		See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416) FOR FURTHER ACTION	
International application No. PCT/EP99/04720	International filing date (day/month/year) 02/07/1999	Priority date (day/month/year) 03/07/1998	
International Patent Classification (IPC) or national classification and IPC H04L29/06			
Applicant NOKIA MOBILE PHONES LIMITED et al.			

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.


2. This REPORT consists of a total of 10 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 14 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand 31/01/2000	Date of completion of this report 11.10.2000
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Köppl, M Telephone No. +49 89 2399 8433



INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/EP99/04720

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

1,4,6-8,11-21	as originally filed			
2,3,5,5a-5b,9, 10	as received on	05/08/2000	with letter of	28/07/2000

Claims, No.:

1-24	as received on	05/08/2000	with letter of	28/07/2000
------	----------------	------------	----------------	------------

Drawings, sheets:

1/2,2/2	as originally filed
---------	---------------------

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

3. ☒ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

see separate sheet

4. Additional observations, if necessary:

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/EP99/04720

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-14, 19-22, 24
	No:	Claims	15-18, 23
Inventive step (IS)	Yes:	Claims	1-12, 19-21
	No:	Claims	15-18, 22-24
Industrial applicability (IA)	Yes:	Claims	1-24
	No:	Claims	

2. Citations and explanations

see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Re Item I

Basis of the report

- 1 The amendments made to claims 1, 5, 14, 19 (corresponding to original claim 13), 22, and 24 go beyond the international application as originally filed.
 - 1.1 In particular, new claims 1, 5, and 19 now contain the formulation "memory means including a separate unit", wherein the memory means forms part of the wireless communication apparatus. This differs from the wording in the respective original claims 1, 5, and 13 where the formulation "a separate unit provided with memory means" was used. Whereas the original wording finds support in the original description, this is not the case for the amended wording since the new wording teach that memory means are present in the wireless communication apparatus and that these memory means in turn include a separate unit. Clearly, the latter feature has not been disclosed in the international application as originally filed, be it explicitly or implicitly having particular regard to figure 2, boxes 16 and 17 (see the International Preliminary Examination Guidelines VI-7.9).
 - 1.2 The additional feature of claim 14 calls for a wireless application apparatus which does not include a smart card, i.e. a separate unit. However, the original description on page 3, line 26 to page 4, line 7 specifies that, according to the invention, a smart card must be present. Claim 14 goes beyond the original disclosure by excision of essential features of the invention (see the International Preliminary Examination Guidelines VI-7.9).
 - 1.3 The subject-matter of claim 22 includes "means for retrieving access information ..." and "means for retrieving a signature ..." which have not been disclosed as such in the international application as originally filed. Rather, the description on page 3, line 26 to page 4, line 7 calls for a separate unit being connected to the wireless communication apparatus, which unit comprises a memory in which is stored control information. Claim 22 goes beyond the original disclosure by excision of essential features of the invention (see the International Preliminary Examination Guidelines VI-7.9).
 - 1.4 The subject-matter of claim 22 includes "memory means provided with information

to control ..." which have not been disclosed as such in the international application as originally filed. Rather, the description on page 3, line 26 to page 4, line 7 calls for a separate unit being connected to the wireless communication apparatus, which unit comprises a memory in which is stored control information. Claim 22 goes beyond the original disclosure by alteration of essential features of the invention (see the International Preliminary Examination Guidelines VI-7.9).

- 2 Therefore, the international preliminary examination report is established as if the amendments had not been made (Rule 70.2 (c) PCT; also see the International Preliminary Examination Guidelines VI-7.8).

Re Item V

Reasoned statement under Rule 66.2 (a) (ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

- 3 Reference is made to the following document:

D1: WO 97 24831 A (MCI COMMUNICATIONS CORPORATION) 10 July 1997

- 4 The subject-matter of claims 1, 5, and 19, as far as their features are disclosed in the international application as originally filed (see Re Item I above), appears to be novel and to involve an inventive step.
- 4.1 Claim 1 concerns a method for establishing a secure connection between a wireless communication apparatus and a data communication apparatus.

Closest prior art is document D1 which describes a communications system, which may also be a wireless communications system, in a which a master key is stored in a smart card.

The subject-matter of claim 1 is based on the problem to provide a master key to a separate unit of a secure communications system.

The problem is solved by having the wireless communication apparatus generate

a master secret code and having it then saved on the separate unit, which is connected to the wireless communication apparatus via contact means.

The solution is not disclosed or suggested by the prior art. Therefore, the subject-matter of claim 1 appears to be novel and to involve an inventive step.

- 4.2 Claim 5 is a representation of method claim 1 in terms of features of a wireless communication apparatus. Therefore, the above arguments with respect to novelty and obviousness of the subject-matter of claim 1 similarly apply to claim 5. Consequently, the subject-matter of claim 5 also appears to be novel and to involve an inventive step.
- 4.3 Claim 19 is a representation of method claim 1 in terms of features of a system for establishing. Therefore, the above arguments with respect to novelty and obviousness of the subject-matter of claim 1 similarly apply to claim 19. Consequently, the subject-matter of claim 19 also appears to be novel and to involve an inventive step.
- 5 Dependent claims 2 to 4, 6 to 13, and 20 to 21 refer to independent claims (as far as these are disclosed; see Re Item I above) which appear to be novel and to involve an inventive step. Therefore, the subject-matter of claims 2 to 4, 6 to 13, and 20 to 21 also appears to be novel and to involve an inventive step.
- 6 The subject-matter of claims 15 (corresponding to original claim 9) and 23 appears not to be novel over the disclosure of document D1 in the sense of Article 33 (2) PCT.
- 6.1 Document D1 discloses, in terms of claim 15, a memory card (see page 4, lines 5 to 9) for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol, arranged to be connected to contact means, provided on said wireless communication apparatus (see page 6, lines 9 to 19), for providing information from the memory card to the wireless communication apparatus, said information is arranged to control the access of the data communication apparatus through a wireless communication network (see page 2, lines 16 to 18), and to save a

calculated master secret related to one or more data communication apparatus, in order to re-establish a secure connection to a data communication apparatus (see page 4, lines 5 to 7).

- 6.2 Since all features of claim 15 are known in combination from document D1, the subject-matter of claim 15 appears not to be novel (Article 33 (2) PCT).
- 6.3 Claim 23 effectively relates to the same subject-matter as claim 15 and differs therefrom only with regard to the definition of the subject-matter or the terminology used (see Re Item VIII below). Therefore, the above arguments regarding lack of novelty of the subject-matter of claim 15 similarly apply to claim 23. Consequently, the subject-matter of claim 23 also appears not to be novel (Article 33 (2) PCT).
- 7 The additional features of claims 16 to 18 do not lead to subject-matter which would appear both to be novel and to involve an inventive step.
- 7.1 The additional feature of claim 16 is also disclosed in document D1 (see page 11, lines 13 to 15, and lines 23 to 26). Therefore, the subject-matter of claim 10 also appears not to be novel.
- 7.2 The additional feature of claim 17 is also disclosed in document D1 (see page 5, lines 3 to 9). Therefore, the subject-matter of claim 11 also appears not to be novel.
- 7.3 The additional feature of claim 18 is also disclosed in document D1 (see page 1, lines 9 to 19). Therefore, the subject-matter of claim 12 also appears not to be novel.
- 8 The subject-matter of claims 14, 22, and 24, as far as their features are disclosed in the international application as originally filed (see Re Item I above), are matters of normal design procedure. Therefore, the subject-matter of claims 14, 22, and 24 appear not to involve an inventive step.
- 9 The industrial applicability of the subject-matter of all the claims is beyond any doubt.

Re Item VII

Certain defects in the international application

- 10 Independent claims 1, 5, 15, 19, and 22 to 24 are not in the two-part form in accordance with Rule 6.3 (b) PCT, which in the present case would be appropriate, with those features known in combination from the prior art document D1 being placed in a preamble (Rule 6.3 (b) (i) PCT) and with the remaining features (in particular the features of generation of a master secret code in the wireless communication apparatus, calculation of the master secret code in the data communication apparatus, and saving the master secret code on the memory means) being included in a characterising part (Rule 6.3 (b) (ii) PCT).
- 11 Reference signs in parentheses should have been inserted in all the claims to increase their intelligibility, Rule 6.2 (b) PCT. This applies to both the preamble and characterising portion (see also PCT International Preliminary Examination Guidelines III-4.11). Where a method claim makes reference to apparatus features, these should also have been accompanied by the respective reference signs wherever appropriate.
- 12 Contrary to the requirements of Rule 5.1 (a) (ii) PCT, the relevant background art disclosed in the document D1 is not mentioned in the description, nor is this document identified therein. The document D1 should therefore have been mentioned in the introductory portion of the description (see also PCT International Preliminary Examination Guidelines II-4.4).

Re Item VIII

Certain observations on the international application

- 13 Although claims 5, 22, and 24, directed to a wireless communication apparatus, respectively, and claims 15 and 23, directed to a memory card, respectively, have been drafted as separate independent claims, they appear to relate effectively to the same subject-matter and to differ from each other only with regard to the definition of the subject-matter for which protection is sought or in respect of the terminology used for the features of that subject-matter. The aforementioned

claims therefore lack conciseness. Moreover, lack of clarity of the claims as a whole arises, since the plurality of independent claims makes it difficult, if not impossible, to determine the matter for which protection is sought, and places an undue burden on others seeking to establish the extent of the protection.

Hence, claims 5, 22, and 24, and claims 15 and 23, do not meet the requirements of Article 6 PCT. An amended set of claims defining the relevant subject-matter in terms of a single independent claim in each category followed by dependent claims covering features which are merely optional should have been filed (Rule 6.4 PCT).

- 14 Claims 1, 5, 19, 22, and 24 are not clear in the sense of Article 6 because they lack an essential feature. According to the description on page 3, line 26 to page 4, line 3, and on page 14, lines 3 to 5, it is an essential feature of the invention that the wireless communication apparatus is provided with contact means. However, this feature is absent from all of claims 1, 5, 19, 22, and 24 rendering them not clear (see also the International Preliminary Examination Guidelines III-4.3). Clear claims should have been filed.
- 15 Claims 1, 5, and 19 are not clear in the sense of Article 6 PCT in that they are not consistent with the description. According to claims 1, 5, and 19, the generation of a master secret code is performed by the wireless communication apparatus. However, according to the description on page 10, line 13 to page 11, line 27 relating to the second and third embodiments of the invention, the generation of the master key is performed in the separate unit, i.e. the smart card (particularly see page 10, lines 16 to 19, and page 11, lines 8 to 14). Therefore, the second and third embodiments do not fall under scope of claims 1, 5, and 19 rendering these claims not clear in the sense of Article 6 PCT (see also the International Preliminary Examination Guidelines III-4.3 "Another form of inconsistency ..."). It should have been indicated in the description that the second and third embodiments are not embodiments according to the invention.
- 16 Claim 5 is not clear in the sense of Article 6 PCT in that it tries to define a wireless communication apparatus using features which do not belong to the apparatus. In particular, claim 5 includes a limitation with respect to the memory means ("... is

provided with information to control the access ...") which does not form part of the apparatus but is only associated with the claimed apparatus when it is in use (see also claim 15 defining the very same feature for the memory card). Clarification would have been required (see also the International Preliminary Examination Guidelines III-4.8a).

- 17 New claim 13 is not clear in the sense of Article 6 PCT because it is formulated as a dependent claim where the base claims are of a different category. Furthermore, claim 13 does not provide an additional teaching whatsoever.

US-A-5,307,411 describe the set up of a secure communication session between two communication units, such as phones or facsimile machines. The secure session is controlled by separate smart cards based verification units associated with a respective one of the communication units. These two
5 verification units exchanges random number, encrypts these numbers by using private keys, returns the encrypted random numbers to their origin. Then the encrypted random number is decrypted based on public keys. If the received numbers corresponds to the transmitted numbers, the parties verifies each other an the secure session may take place. However, this requires that
10 both communication units are provided with a smart card reader, which is not a necessary requirement in a server, like e.g. an Internet server. Thus, this document is quite restricting for the user, since it requires that both parties have a smart card reader, and is less suitable for communication between a wireless communication apparatus and a data communication apparatus.
15 Also, every time a session is going to be established between the two communication apparatuses, an exchange of keys must be done.

Also, US-A-5,371,794, by Sun Microsystems, discloses a way to providing a secure wireless communication link between a mobile nomadic device and a
20 base computing unit. The mobile device sends a host certificate to the base along with a randomly chosen challenge value (CH1) and a list of supported shared key algorithms. The base sends random number (RN1) encrypted in the mobile's public key and an identifier for the chosen algorithm back to the mobile. The base saves the RN1 value and adds the CH1 value and the
25 chosen algorithm to the mobile. The mobile verifies under the public key of the base the signature on the message. When the public key is verified, the mobile determines the value of RN1 by decrypting the public key under the private key of the mobile. The mobile then generates RN2 and a session key, and encrypts RN2 under the public key of the base to the base. The base
30 verifies and decrypting the RN2, and determines the session key. Finally, the

mobile and the base can enter a data transfer phase using encrypted data which is decrypted using the session key which is $RN1 + RN2$. The values of $RN1$ and $RN2$ are always derived from the last key exchange, which may be from the initial connection setup or from the last key change message, whichever is more recent. This means that each time a data transfer is made, two new numbers is generated based on $RN1$ and $RN2$, which will make the data transfer quite slow. Thus, as in US-A-5,307,411, every time a session is going to be established between the two apparatuses, in this case the mobile nomadic device and the base computing unit, an exchange of keys must be done.

Summary of the Invention

The main object of the present invention is to establish a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol.

Another object is to enable the user to re-establish a secure at a later occasion, since establishing a secure connection is a heavy procedure both computationally and due to intensive data transfer. That is why, there is a need to use the mutually agreed master secret for a relatively long time. The problem is to store the master key in a secure way. Partly due to that problem, it is common practice to restrict the lifecycle of the master secret and the associated secure session to e.g., 24 hours, after which it is required to perform the heavy key establishment procedure a new.

25

The main object is achieved in accordance with the present invention by connecting a wireless communication apparatus, e.g. a cellular phone, to a separate unit, e.g. a smart card, a SIM (Subscriber Identity Module) card, etc., which may store sensitive data of a secure connection. This means that the wireless communication apparatus having some kind of contact means, for

30

5

comprising the public key, it will generate a master secret code, and calculates a signature based on the chosen algorithm, the public key and the master secret code. Thereafter, the wireless communication apparatus will transmit a respond to the data communication apparatus. This respond
5 comprises the calculated signature. When the data communication apparatus receives the respond, comprising the signature, it will calculate the master secret code based on the chosen algorithm, the signature received, and the private key. Finally, the data communication apparatus will be able to establish a secure connection to the wireless communication apparatus.

10

Further advantages of the vane arrangement according to the present invention will be apparent from the dependent claims.

15

Brief Description of the Drawing

Fig. 1 schematically illustrates a preferred embodiment of a hand portable phone according to the invention.

20

Fig. 2 schematically shows the essential parts of a telephone for communication with a cellular or cordless network.

Fig. 3 schematically shows how the secure session is set up between a client
25 /phone and a server according to the invention.

Fig. 4 illustrates the message structure for setting up a secure connection according to the invention.

Detailed Description of Embodiments

30

during long-living WTLS sessions. Finally the memory of the smart card 16 is used for recording the level security of the sessions. According to the invention the WTLS support in a smart card 16 can be described with reference to the following three embodiments.

5

First embodiment.

According to this embodiment, the smart card 16 is used for storage of permanent, typically certified, private keys and for performing operations using these keys. The operations includes signing operation (e.g., ECDSA or
10 RSA) for client authentication when needed for the selected handshake scheme; key exchange operation using a fixed client key (e.g., ECDH key, in ECDH_ECDSA handshake).

The smart card 16 is not required to perform the calculation of the master
15 secret or operations using the master key. These calculations may advantageously be performed by the controller 18 of the phone. However, the smart card 16 may act as a persistent storage for WTLS secure session (and connection) data, including master secrets. In this case, master secrets would be calculated and used for key derivation in the volatile phone memory (the
20 RAM 17a) but erased from there when not needed at that moment, e.g., when the user exits from secure WAP applications. Not storing session data persistently in phone 1 may improve security, e.g., in the case of a stolen phone 1. It also brings better usability in the case of changing the smart card 16 from one phone 1 to another.

25

Additionally, for portability, the smart card 16 may store needed certificates. Storage of trusted root certificates (or public keys) has significance also from security point of view: they must not be altered - but they can be exposed without danger.

30

Note that when public key encryption based key exchange (e.g., RSA) is used according to the first embodiment of the invention, there is no advantage in doing public key encryption on the smart card 16 when the pre-master secret would anyway be returned to the phone1, for master secret calculation in the controller 18.

When client authentication is not supported in WTLS, at the minimum, the smart card 16 only acts as a storage for session data. If client authentication is supported, the card would be able to perform a signing operation based on a private key (e.g., ECDSA or RSA) stored in the card, or key agreement calculation (e.g., ECDH) based on a fixed key stored in the card.

Second embodiment.

According to the second embodiment, the smart card 16 is used as a tamper resistant device for all crypto-critical functionality: storage of all persistent keys and operations using these keys. Besides the operations performed according to the first embodiment, the smart card 16 now also supports the calculation (ECDH key exchange) or generation (RSA key exchange) of the pre-master secret; calculation and storage of the master secret for each secure session; and derivation and output of key material (for MAC, encryption keys, IV, finished check), based on the master secret

The phone 1 stores MAC and message encryption keys as long as they are currently needed. These keys have a limited lifetime which may be negotiated during the WTLS handshake - in the extreme case they are used for a single message only. The phone 1 has to delete the from its RAM memory 17a when the user exits from the secure WAP applications. These keys can always be derived anew from the master secret if needed.

CLAIMS

1. Method for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on
5 a wireless application protocol, wherein said wireless communication apparatus having contact means for receiving information from a separate unit provided with memory means, said memory means comprising information to control the access of the wireless communication apparatus through a wireless communication network connected to said data
10 communication apparatus, comprising the following steps:
- connecting said wireless communication apparatus to the separate unit, accessing the wireless communication network connected to said data communication apparatus
 - the wireless communication apparatus transmits a request to the data
15 communication apparatus to establish a connection, said request comprising information of which pre-defined algorithm(s) the wireless communication apparatus supports,
 - upon reception of said request, the data communication apparatus choose at least one algorithm, associated with a public key and a
20 private key, and transmits a message back to the wireless communication apparatus, said message comprising the public key and information about which algorithm the data communication apparatus has chosen,
 - upon reception of the message, comprising the public key, the wireless
25 communication apparatus generates a master secret code, and calculates a signature based on the chosen algorithm, the public key and the master secret code, and transmits a respond to the data communication apparatus, said respond comprising the calculated signature,

- upon reception of the respond comprising the signature, the data communication apparatus calculates the master secret code based on the chosen algorithm, the signature received and the private key, and establish a secure connection to the wireless communication apparatus, and
 - saving said master secret code on said memory means and in the data communication apparatus, in order to re-establish the connection at a later occasion.
2. A method according to claim 1, and comprising a step of saving said master secret under a pre-defined time.
3. A method according to claim 1 or 2, and comprising a step of re-establishing the connection by
- transmitting a request from the wireless communication apparatus to the data communication apparatus, said request comprising the calculated signature based on the chosen algorithm, the public key and the stored secret key, and
 - upon reception of the request, the data communication apparatus calculates the master secret code based on the chosen algorithm, the signature received, and the private key, and, establish a secure connection to the wireless communication apparatus.
4. A method according to claim 1, 2, or 3, and comprising a step of providing said memory means in a smart card.
5. Wireless communication apparatus for establishing a secure connection to a data communication apparatus based on a wireless application protocol, said wireless communication apparatus comprising:

24

- communication means for establishing a connection to a wireless communication network connected to said data communication apparatus,
- 5 - contact means for receiving information from a separate unit provided with memory means, said memory means is provided with information to control the access of the data communication apparatus through the wireless communication network,
- 10 - reading means for reading information received from the data communication apparatus and the information provided on said memory means,
- random generating means, for generating a master secret code,
- pre-defined algorithm(s), to generate a signature based on said master secret code and a public key received from said data communication apparatus, which is to be used when the wireless communication apparatus is going to establish a secure connection to the data communication apparatus, and
- 15 - said reading means comprising a secure database provided with at least one master secret code and/or at least one signature related to one or more data communication apparatus, in order to re-establish a
- 20 secure connection to a data communication apparatus.

6. A wireless communication apparatus according to claim 5, having its memory means exchangeable.
- 25 7. An apparatus according to claim 5 or 6, said memory means is a smart card.
8. An apparatus according to claim 5, 6, or 7, said memory means is a subscriber identity module.

30

9. Memory card for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol, arranged to be connected to said wireless communication apparatus having contact means for receiving information from the memory card, and said memory card is provided with information to control the access of the data communication apparatus through a wireless communication network.
10. A memory card according to claim 9, further comprising encryption means for encrypting the master secret, which is to be used as a signature for the wireless communication apparatus when it is establishing a secure connection.
11. A memory card according to claim 9 or 10, comprising a secure database provided with at least one master secret code and/or at least one signature related to one or more data communication apparatus, in order to re-establish a secure connection to a data communication apparatus.
12. A memory card according to claim 9, 10, or 11, is provided on a smart card.
13. System for establishing a secure connection when using a wireless application protocol, comprising:
- a data communication apparatus based on the wireless application protocol,
 - a wireless communication network, connected to said data communication apparatus,
 - a wireless communication apparatus having contact means for receiving information from a separate unit provided with memory means, and

- the separate unit provided with the memory means, said memory means, comprising information to control the access of the wireless communication apparatus through the wireless communication network, wherein
- 5 - the wireless communication apparatus is arranged to transmit a request to the data communication apparatus to establish a connection, said request comprising information of which pre-defined algorithm(s) the wireless communication apparatus supports,
- 10 - upon reception of said request, the data communication apparatus is arranged to choose at least one algorithm, associated with a public key and a private key, and to transmit a message back to the wireless communication apparatus, said message comprising the public key and information about which algorithm the data communication apparatus will choose,
- 15 - upon reception of said message, comprising the public key, the wireless communication apparatus is arranged to generate a master secret code, to calculate a signature based on the chosen algorithm, the public key and the master secret code, and to transmit a respond to the data communication apparatus, said respond comprising the
- 20 calculated signature,
- upon reception of the respond comprising the signature, the data communication apparatus is arranged to calculate the master secret code based on the chosen algorithm, the signature received, and the private key, and, thus establish a secure connection to the wireless
- 25 communication apparatus, and
- said memory means and the data communication apparatus are arranged to save said master secret code, in order to re-establish the connection at a later occasion.

27

14. A system according to claim 13, said master secret is arranged to be saved under a pre-defined time.

5 15. A system according to claim 13, or 14, said memory means is a smart card.

09/720971

528 Rec'd PCT/PTO 03 JAN 2001

2

US-A-5,307,411 describes the set up of a secure communication session between two communication units, such as phones or facsimile machines. The secure session is controlled by separate smart cards based verification units associated with a respective one of the communication units. These two

5 verification units exchange random number, encrypt these numbers by using private keys, and return the encrypted random numbers to their origin. Then the encrypted random number is decrypted based on public keys. If the received numbers correspond to the transmitted numbers, the parties verify each other and the secure session may take place. However, this requires

10 that both communication units are provided with a smart card reader, which is not a necessary requirement in a server, like e.g. an Internet server. Thus, this document is quite restricting for the user, since it requires that both parties have a smart card reader, and is less suitable for communication between a wireless communication apparatus and a data communication

15 apparatus. Also, every time a session is going to be established between the two communication apparatuses, an exchange of keys must be done.

Also, US-A-5,371,794, by Sun Microsystems, discloses a way to providing a secure wireless communication link between a mobile nomadic device and a

20 base computing unit. The mobile device sends a host certificate to the base along with a randomly chosen challenge value (CH1) and a list of supported shared key algorithms. The base sends random number (RN1) encrypted in the mobile's public key and an identifier for the chosen algorithm back to the mobile. The base saves the RN1 value and adds the CH1 value and the

25 chosen algorithm to the mobile. The mobile verifies under the public key of the base the signature on the message. When the public key is verified, the mobile determines the value of RN1 by decrypting the public key under the private key of the mobile. The mobile then generates RN2 and a session key, and encrypts RN2 under the public key of the base to the base. The base

30 verifies and decrypting the RN2, and determines the session key. Finally, the

mobile and the base can enter a data transfer phase using encrypted data which is decrypted using the session key which is $RN1 + RN2$. The values of $RN1$ and $RN2$ are always derived from the last key exchange, which may be from the initial connection setup or from the last key change message, whichever is more recent. This means that each time a data transfer is made, two new numbers are generated based on $RN1$ and $RN2$, which will make the data transfer quite slow. Thus, as in US-A-5,307,411, every time a session is going to be established between the two apparatuses, in this case the mobile nomadic device and the base computing unit, an exchange of keys must be done.

Summary of the Invention

The main object of the present invention is to establish a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol.

Another object is to enable the user to re-establish a secure connection at a later occasion, since establishing a secure connection is a heavy procedure both computationally and due to intensive data transfer. That is why, there is a need to use the mutually agreed master secret for a relatively long time. The problem is to store the master key in a secure way. Partly due to that problem, it is common practice to restrict the lifecycle of the master secret and the associated secure session to e.g., 24 hours, after which it is required to perform the heavy key establishment procedure anew.

25

The main object is achieved in accordance with the present invention by connecting a wireless communication apparatus, e.g. a cellular phone, to a separate unit, e.g. a smart card, a SIM (Subscriber Identity Module) card, etc., which may store sensitive data of a secure connection. This means that the wireless communication apparatus having some kind of contact means, for

30

comprising the public key, it will generate a master secret code, and calculates a signature based on the chosen algorithm, the public key and the master secret code. Thereafter, the wireless communication apparatus will transmit a respond to the data communication apparatus. This respond
5 comprises the calculated signature. When the data communication apparatus receives the respond, comprising the signature, it will calculate the master secret code based on the chosen algorithm, the signature received, and the private key. Finally, the data communication apparatus will be able to establish a secure connection to the wireless communication apparatus.

10

In accordance with a first aspect of the present invention there is provided a method for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol, wherein said wireless communication apparatus
15 has memory means including a separate unit comprising information to control the access of the wireless communication apparatus through a wireless communication network connected to said data communication apparatus, comprising the following steps: connecting said wireless communication apparatus to the separate unit, accessing the wireless
20 communication network connected to said data communication apparatus the wireless communication apparatus transmits a request to the data communication apparatus to establish a connection, said request comprising information of which pre-defined algorithm(s) the wireless communication apparatus supports, upon reception of said request, the data communication
25 apparatus chooses at least one algorithm associated with a public and a private key, and transmits a message back to the wireless communication apparatus, said message comprising the public key and information about which algorithm the data communication apparatus has chosen, upon reception of the message, comprising the public key, the wireless
30 communication apparatus generates a master secret code, and calculates a

Sa

signature based on the chosen algorithm, the public key and the master secret code, and transmits a response to the data communication apparatus, said response comprising the calculated signature, upon reception of the respond comprising the signature, the data communication apparatus
5 calculates the master secret code based on the chosen algorithm, the signature received and the private key, and establish a secure connection to the wireless communication apparatus, and saving said master secret code on said memory means and in the data communication apparatus, in order to re-establish the connection at a later occasion.

10

According to a second aspect of the present invention there is provided wireless communication apparatus for establishing a secure connection to a data communication apparatus based on a wireless application protocol, said wireless communication apparatus comprising: communication means for
15 establishing a connection to a wireless communication network connected to said data communication apparatus, memory means including a separate unit provided with information to control the access of the data communication apparatus through the wireless communication network, means for generating a master secret code control means arranged to use a pre-defined
20 algorithm(s) for generating a signature based on said master secret code and a public key received from said data communication apparatus, for use when the wireless communication apparatus establishes a secure connection to the data communication apparatus, said memory means comprising a secure database for storing at least one master secret code and/or at least one
25 signature related to one or more data communication apparatus, in order to re-establish a secure connection to a data communication apparatus.

According to a third aspect of the present invention there is provided memory
30 apparatus and a data communication apparatus based on a wireless

5b

- application protocol, arranged to be connected to contact means, provided on said wireless communication apparatus, for providing information from the memory card to the wireless communication apparatus upon establishing a secure session to a data communication apparatus, said information is
- 5 arranged to control the access of the data communication apparatus through a wireless communication network, and to save a calculated master secret related to one or more data communication apparatus, in order to re-establish a secure connection to a data communication apparatus.
- 10 Further advantages of the vane arrangement according to the present invention will be apparent from the dependent claims.

Brief Description of the Drawing

- 15 Fig. 1 schematically illustrates a preferred embodiment of a hand portable phone according to the invention.

Fig. 2 schematically shows the essential parts of a telephone for communication with a cellular or cordless network.

20

Fig. 3 schematically shows how the secure session is set up between a client /phone and a server according to the invention.

- Fig. 4 illustrates the message structure for setting up a secure connection
- 25 according to the invention.

Detailed Description of Embodiments

a

during long-living WTLS sessions. Finally the memory of the smart card 16 is used for recording the level security of the sessions. According to the invention the WTLS support in a smart card 16 can be described with reference to the following three embodiments.

5

First embodiment.

According to this embodiment, the smart card 16 is used for storage of permanent, typically certified, private keys and for performing operations using these keys. The operations include signing operations (e.g., ECDSA or
10 RSA) for client authentication when needed for the selected handshake scheme; key exchange operations using a fixed client key (e.g., ECDH key, in ECDH_ECDSA handshake).

The smart card 16 is not required to perform the calculation of the master
15 secret or operations using the master key. These calculations may advantageously be performed by the controller 18 of the phone. However, the smart card 16 may act as a persistent storage for WTLS secure session (and connection) data, including master secrets. In this case, master secrets would be calculated and used for key derivation in the volatile phone memory (the
20 RAM 17a) but erased from there when not needed at that moment, e.g., when the user exits from secure WAP applications. Not storing session data persistently in phone 1 may improve security, e.g., in the case of a stolen phone 1. It also brings better usability in the case of changing the smart card 16 from one phone 1 to another.

25

Additionally, for portability, the smart card 16 may store needed certificates. Storage of trusted root certificates (or public keys) has significance also from security point of view: they must not be altered - but they can be exposed without danger.

30

10

Note that when public key encryption based key exchange (e.g., RSA) is used according to the first embodiment of the invention, there is no advantage in doing public key encryption on the smart card 16 when the pre-master secret would anyway be returned to the phone 1, for master secret calculation in the
5 controller 18.

When client authentication is not supported in WTLS, at the minimum, the smart card 16 only acts as a storage for session data. If client authentication is supported, the card would be able to perform a signing operation based on
10 a private key (e.g., ECDSA or RSA) stored in the card, or key agreement calculation (e.g., ECDH) based on a fixed key stored in the card.

Second embodiment.

According to the second embodiment, the smart card 16 is used as a tamper
15 resistant device for all crypto-critical functionality: storage of all persistent keys and operations using these keys. Besides the operations performed according to the first embodiment, the smart card 16 now also supports the calculation (ECDH key exchange) or generation (RSA key exchange) of the pre-master secret; calculation and storage of the master secret for each
20 secure session; and derivation and output of key material (for MAC, encryption keys, IV, finished check), based on the master secret

The phone 1 stores MAC and message encryption keys as long as they are currently needed. These keys have a limited lifetime which may be negotiated
25 during the WTLS handshake - in the extreme case they are used for a single message only. The phone 1 has to delete the from its RAM memory 17a when the user exits from the secure WAP applications. These keys can always be derived anew from the master secret if needed.

23

CLAIMS

1. Method for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol, wherein said wireless communication apparatus has memory means including a separate unit comprising information to control the access of the wireless communication apparatus through a wireless communication network connected to said data communication apparatus, comprising the following steps:
- connecting said wireless communication apparatus to the separate unit, accessing the wireless communication network connected to said data communication apparatus
- the wireless communication apparatus transmits a request to the data communication apparatus to establish a connection, said request comprising information of which pre-defined algorithm(s) the wireless communication apparatus supports,
- upon reception of said request, the data communication apparatus chooses at least one algorithm associated with a public and a private key, and transmits a message back to the wireless communication apparatus, said message comprising the public key and information about which algorithm the data communication apparatus has chosen,
- upon reception of the message, comprising the public key, the wireless communication apparatus generates a master secret code, and calculates a signature based on the chosen algorithm, the public key and the master secret code, and transmits a response to the data communication apparatus, said response comprising the calculated signature,
- upon reception of the response comprising the signature, the data communication apparatus calculates the master secret code based on the

23

chosen algorithm, the signature received and the private key, and establish a secure connection to the wireless communication apparatus, and saving said master secret code on said memory means and in the data communication apparatus, in order to re-establish the connection at a later
5 occasion.

2. A method according to claim 1, and comprising a step of saving said master secret under a pre-defined time.

10 3. A method according to claim 1 or 2, and comprising a step of re-establishing the connection by transmitting a request from the wireless communication apparatus to the data communication apparatus, said request comprising the calculated signature based on the chosen algorithm, the public key and the stored secret key, and
15 upon reception of the request, the data communication apparatus calculates the master secret code based on the chosen algorithm, the signature received, and the private key, and, establish a secure connection to the wireless communication apparatus.

20 4. A method according to claim 1, 2, or 3, and comprising a step of providing said separate unit in a smart card.

5. Wireless communication apparatus for establishing a secure connection to a data communication apparatus based on a wireless
25 application protocol, said wireless communication apparatus comprising: communication means for establishing a connection to a wireless communication network connected to said data communication apparatus, memory means including a separate unit provided with information to control the access of the data communication apparatus through the wireless
30 communication network,

24
26

- means for generating a master secret code
- control means arranged to use a pre-defined algorithm(s) for generating a signature based on said master secret code and a public key received from said data communication apparatus, for use when the wireless
- 5 communication apparatus establishes a secure connection to the data communication apparatus,
- said memory means comprising a secure database for storing at least one master secret code and/or at least one signature related to one or more data communication apparatus, in order to re-establish a secure connection to a
- 10 data communication apparatus.
6. A wireless communication apparatus according to claim 5, having its memory means exchangeable.
- 15 7. Wireless communication apparatus according to claim 5 or 6 wherein the master secret code is stored on the separate unit.
8. Wireless communication apparatus according to any one of claims 5 to 7 wherein the signature is stored on the separate unit.
- 20 9. Wireless communication apparatus according to any one of claims 5 to 8 wherein the master secret code is generated on the separate unit.
10. Wireless communication apparatus according to any one of claims 5 to 25 9 wherein the signature is generated on the separate unit.
11. Wireless communication apparatus according to any one of claims 5 to 10 wherein the separate unit comprises a smart card.

25

12. An apparatus according to claim 11 wherein the smart card is a subscriber identity module.

13. A smart card according to claims 11 or 12.

5

14. A wireless communication apparatus according to any one of claims 5 to 12 without the smart card of claim 13.

15. Memory card for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol, arranged to be connected to contact means, provided on said wireless communication apparatus, for providing information from the memory card to the wireless communication apparatus upon establishing a secure session to a data communication apparatus, said information is arranged to control the access of the data communication apparatus through a wireless communication network, and to save a calculated master secret related to one or more data communication apparatus, in order to re-establish a secure connection to a data communication apparatus.

20

16. A memory card according to claim 15, further comprising encryption means for encrypting the master secret, which is to be used as a signature for the wireless communication apparatus when it is establishing a secure connection.

25

17. A memory card according to claim 15 or 16, comprising a secure database provided with at least one master secret code and/or at least one signature related to one or more data communication apparatus, in order to re-establish a secure connection to a data communication apparatus.

30

26

18. A memory card according to claim 15, 16, or 17, is provided on a smart card.

19. System for establishing a secure connection when using a wireless application protocol, comprising:
- 5 a data communication apparatus based on the wireless application protocol, a wireless communication network, connected to said data communication apparatus,
- 10 a wireless communication apparatus having memory means including a separate unit comprising information to control the access of the wireless communication apparatus through the wireless communication network, wherein
- 15 the wireless communication apparatus is arranged to transmit a request to the data communication apparatus to establish a connection, said request comprising information of which pre-defined algorithm(s) the wireless communication apparatus supports,
- upon reception of said request, the data communication apparatus is arranged to choose at least one algorithm, associated with a public key and a private key, and to transmit a message back to the wireless communication
- 20 apparatus, said message comprising the public key and information about which algorithm the data communication apparatus will choose,
- upon reception of said message, comprising the public key, the wireless communication apparatus is arranged to generate a master secret code, to calculate a signature based on the chosen algorithm, the public key and the
- 25 master secret code, and to transmit a respond to the data communication apparatus, said respond comprising the calculated signature,
- upon reception of the respond comprising the signature, the data communication apparatus is arranged to calculate the master secret code based on the chosen algorithm, the signature received, and the private key,

27

and, thus establish a secure connection to the wireless communication apparatus, and

said memory means being arranged to save said master secret code, in order to re-establish the connection at a later occasion.

5

20. A system according to claim 19, said master secret is arranged to be saved under a pre-defined time.

10

21. A system according to claim 19, or 20, said memory means is a smart card.

15

22. A wireless communication apparatus for establishing a secure connection to a data communication apparatus through a wireless network based on a wireless application protocol, said wireless communication apparatus comprising:

means for establishing a connection with the data communication apparatus through the wireless network

20

means for retrieving access information including which of a set of pre-defined algorithms is supported, for transmission to the data communication apparatus;

means for processing information including a public key and the selection of one of the supported algorithms received from the data communication apparatus for storage;

25

means for retrieving a signature based on a generated master secret code and the public key received from the data communication apparatus; and means for utilising the signature and/or the master secret key during communication with the data communication apparatus in order to re-establish a secure connection.

28

23. A memory card for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol comprising contact means for cooperation with the wireless communication apparatus

- 5 a memory for storing a master secret code associated with the data communication apparatus and responsive to a request from the wireless communication apparatus to provide such code for utilisation of the master secret key during communication with the data communication apparatus in order to re-establish a secure connection.

10

24. Wireless communication apparatus for establishing a secure connection to a data communication apparatus based on a wireless application protocol, said wireless communication apparatus comprising:

- 15 communication means for establishing a connection to a wireless communication network connected to said data communication apparatus, memory means provided with information to control the access of the data communication apparatus through the wireless communication network upon establishing a secure session to a data communication apparatus, reading means for reading information received from the data communication
- 20 apparatus and the information provided on said memory means, means for generating a master secret code, control means arranged to use a pre-defined algorithm(s) for generating a signature based on said master secret code and a public key received from said data communication apparatus, which is to be used when the wireless
- 25 communication apparatus is going to establish a secure connection to the data communication apparatus, and said reading means comprising a secure database provided with at least one master secret code and/or at least one signature related to one or more data communication apparatus, in order to re-establish a secure connection to a
- 30 data communication apparatus.

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:

Higgin, Paul
NOKIA IPR DEPARTMENT
Nokia House, Summit Avenue
Southwood
Farnborough
Hampshire GU14 0NG
GRANDE BRETAGNE

☐ Comp Record☐ File Record☐ ☐ ☐ ☐

16 OCT 2000

☐ Renewal Record☐ Citations☐ Inv Award

PCT

NOTIFICATION OF TRANSMITTAL OF
THE INTERNATIONAL PRELIMINARY
EXAMINATION REPORT

(PCT Rule 71.1)

☐ Letters

☐ Date of mailing
(day/month/year)

11.10.2000

Applicant's or agent's file reference

PAT 98502PCT

IMPORTANT NOTIFICATION

International application No.
PCT/EP99/04720

International filing date (day/month/year)
02/07/1999

Priority date (day/month/year)
03/07/1998

Applicant

NOKIA MOBILE PHONES LIMITED et al.

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.
2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.
3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. REMINDER

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/

 European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Authorized officer

Ahrens, R

Tel. +49 89 2399-8136



PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

To:
NOKIA IPR DEPARTMENT
Nokia House
Attn. Higgin, Paul
Summit Avenue
Farnborough
Hampshire GU14 0NG
UNITED KINGDOM

☒ Comp Record
☒ File Record
☒ ☐ Div

07 DEC 1999

☐ Renewal Record
☒ Citations
☐ Inv Award

NOTIFICATION OF TRANSMITTAL OF
THE INTERNATIONAL SEARCH REPORT
OR THE DECLARATION

(PCT Rule 44.1)

☒ Letters

Date of mailing
(day/month/year)

03/12/1999

Applicant's or agent's file reference

PAT 98502PCT

FOR FURTHER ACTION

See paragraphs 1 and 4 below

International application No.

PCT/EP 99/04720

International filing date
(day/month/year)

02/07/1999

Applicant

NOKIA MOBILE PHONES LIMITED et al.

1. ☒ The applicant is hereby notified that the International Search Report has been established and is transmitted herewith.

Filing of amendments and statement under Article 19:

The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

When? The time limit for filing such amendments is normally 2 months from the date of transmittal of the International Search Report; however, for more details, see the notes on the accompanying sheet.

Where? Directly to the International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Facsimile No.: (41-22) 740.14.35

For more detailed instructions, see the notes on the accompanying sheet.

2. ☐ The applicant is hereby notified that no International Search Report will be established and that the declaration under Article 17(2)(a) to that effect is transmitted herewith.

3. ☐ With regard to the protest against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Further action(s):** The applicant is reminded of the following:

Shortly after 18 months from the priority date, the international application will be published by the International Bureau.

If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90bis.1 and 90bis.3, respectively, before the completion of the technical preparations for international publication.

Within 19 months from the priority date, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later).

Within 20 months from the priority date, the applicant must perform the prescribed acts for entry into the national phase before all designated Offices which have not been elected in the demand or in a later election within 19 months from the priority date or could not be elected because they are not bound by Chapter II.

Name and mailing address of the International Searching Authority



European Patent Office, P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Theresia Van Deursen

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the PCT Applicant's Guide, a publication of WIPO.

In these Notes, "Article", "Rule", and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only.

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When?

Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How?

Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Administrative Instructions, Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

NOTES TO FORM PCT/ISA/220 (continued)

The letter must indicate the differences between the claims as filed and the claims as amended. It must, in particular, indicate, in connection with each claim appearing in the international application (it being understood that identical indications concerning several claims may be grouped), whether

- (i) the claim is unchanged;
- (ii) the claim is cancelled;
- (iii) the claim is new;
- (iv) the claim replaces one or more claims as filed;
- (v) the claim is the result of the division of a claim as filed.

The following examples illustrate the manner in which amendments must be explained in the accompanying letter:

1. [Where originally there were 48 claims and after amendment of some claims there are 51]:
"Claims 1 to 29, 31, 32, 34, 35, 37 to 48 replaced by amended claims bearing the same numbers; claims 30, 33 and 36 unchanged; new claims 49 to 51 added."
2. [Where originally there were 15 claims and after amendment of all claims there are 11]:
"Claims 1 to 15 replaced by amended claims 1 to 11."
3. [Where originally there were 14 claims and the amendments consist in cancelling some claims and in adding new claims]:
"Claims 1 to 6 and 14 unchanged; claims 7 to 13 cancelled; new claims 15, 16 and 17 added." or
"Claims 7 to 13 cancelled; new claims 15, 16 and 17 added; all other claims unchanged."
4. [Where various kinds of amendments are made]:
"Claims 1-10 unchanged; claims 11 to 13, 18 and 19 cancelled; claims 14, 15 and 16 replaced by amended claim 14; claim 17 subdivided into amended claims 15, 16 and 17; new claims 20 and 21 added."

"Statement under article 19(1)" (Rule 46.4)

The amendments may be accompanied by a statement explaining the amendments and indicating any impact that such amendments might have on the description and the drawings (which cannot be amended under Article 19(1)).

The statement will be published with the international application and the amended claims.

It must be in the language in which the international application is to be published.

It must be brief, not exceeding 500 words if in English or if translated into English.

It should not be confused with and does not replace the letter indicating the differences between the claims as filed and as amended. It must be filed on a separate sheet and must be identified as such by a heading, preferably by using the words "Statement under Article 19(1)."

It may not contain any disparaging comments on the international search report or the relevance of citations contained in that report. Reference to citations, relevant to a given claim, contained in the international search report may be made only in connection with an amendment of that claim.

Consequence if a demand for international preliminary examination has already been filed

If, at the time of filing any amendments under Article 19, a demand for international preliminary examination has already been submitted, the applicant must preferably, at the same time of filing the amendments with the International Bureau, also file a copy of such amendments with the International Preliminary Examining Authority (see Rule 62.2(a), first sentence).

Consequence with regard to translation of the international application for entry into the national phase

The applicant's attention is drawn to the fact that, where upon entry into the national phase, a translation of the claims as amended under Article 19 may have to be furnished to the designated/elected Offices, instead of, or in addition to, the translation of the claims as filed.

For further details on the requirements of each designated/elected Office, see Volume II of the PCT Applicant's Guide.

PCT REQUEST

PAT 98502PCT

Original (for SUBMISSION) - printed on 01.07.1999 01:08:25 PM

0	For receiving Office use only	
0-1	International Application No.	
0-2	International Filing Date	
0-3	Name of receiving Office and "PCT International Application"	
0-4	Form - PCT/RO/101 PCT Request Prepared using	PCT-EASY Version 2.84 (updated 01.06.1999)
0-5	Petition The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	Receiving Office (specified by the applicant)	European Patent Office (EPO) (RO/EP)
0-7	Applicant's or agent's file reference	PAT 98502PCT
I	Title of invention	SECURE SESSION SET UP BASED ON THE WIRELESS APPLICATION PROTOCOL
II	Applicant	
II-1	This person is:	applicant only
II-2	Applicant for	all designated States except US
II-4	Name	NOKIA MOBILE PHONES LIMITED
II-5	Address:	KEILALAHDENTIE 4 FIN-02150 ESPOO Finland
II-6	State of nationality	FI
II-7	State of residence	FI
II-8	Telephone No.	+358 24 3061
II-9	Facsimile No.	+358 24 30 64544
III-1	Applicant and/or inventor	
III-1-1	This person is:	applicant and inventor
III-1-2	Applicant for	US only
III-1-4	Name (LAST, First)	IMMONEN, Olli
III-1-5	Address:	TUOHUSKUJA 16 A 5 FIN-00670 HELSINKI Finland
III-1-6	State of nationality	FI
III-1-7	State of residence	FI

PCT REQUEST

2/4

Original (for SUBMISSION) - printed on 01.07.1999 01:08:25 PM

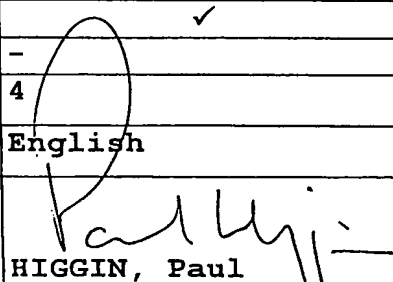
PAT 98502PCT

IV-1	Agent or common representative; or address for correspondence The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	agent
IV-1-1	Name (LAST, First)	HIGGIN, Paul
IV-1-2	Address:	NOKIA HOUSE SUMMIT AVENUE SOUTHWOOD FARNBOROUGH, Hampshire GU14 ONG United Kingdom
IV-1-3	Telephone No.	+44 1252 865000
IV-1-4	Facsimile No.	+44 1252 865080
IV-2	Additional agent(s)	additional agent(s) with same address as first named agent
IV-2-1	Name(s)	JEFFERY, Kendra; HIBBERT, Juliet; FRAIN, Timothy; MUIR, Henry; HAWS, Helen
V	Designation of States	
V-1	Regional Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	AP: GH GM KE LS MW SD SL SZ UG ZW and any other State which is a Contracting State of the Harare Protocol and of the PCT EA: AM AZ BY KG KZ MD RU TJ TM and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE and any other State which is a Contracting State of the European Patent Convention and of the PCT OA: BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG and any other State which is a member State of OAPI and a Contracting State of the PCT
V-2	National Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	AE AL AM AT AU AZ BA BB BG BR BY CA CH&LI CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZA ZW

PCT REQUEST

PAT 98502PCT

Original (for SUBMISSION) - printed on 01.07.1999 01:08:25 PM

V-5	Precautionary Designation Statement In addition to the designations made under items V-1, V-2 and V-3, the applicant also makes under Rule 4.9(b) all designations which would be permitted under the PCT except any designation(s) of the State(s) indicated under Item V-6 below. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit.	
V-6	Exclusion(s) from precautionary designations	NONE
VI-1	Priority claim of earlier national application	
VI-1-1	Filing date	03 July 1998 (03.07.1998)
VI-1-2	Number	867/98
VI-1-3	Country	DK
VII-1	International Searching Authority Chosen	European Patent Office (EPO) (ISA/EP)
VIII	Check list	number of sheets electronic file(s) attached
VIII-1	Request	4 -
VIII-2	Description	21 -
VIII-3	Claims	6 -
VIII-4	Abstract	1 p98502pct.txt
VIII-5	Drawings	2 -
VIII-7	TOTAL	34
	Accompanying items	paper document(s) attached electronic file(s) attached
VIII-8	Fee calculation sheet	✓ -
VIII-9	Separate signed power of attorney	✓ -
VIII-16	PCT-EASY diskette	- diskette
VIII-18	Figure of the drawings which should accompany the abstract	4
VIII-19	Language of filing of the international application	English
IX-1	Signature of applicant or agent	
IX-1-1	Name (LAST, First)	HIGGIN, Paul 11/7/99

FOR RECEIVING OFFICE USE ONLY

10-1	Date of actual receipt of the purported international application	
10-2	Drawings:	
10-2-1	Received	
10-2-2	Not received	
10-3	Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application	
10-4	Date of timely receipt of the required corrections under PCT Article 11(2)	

PCT REQUEST

PAT 98502PCT

Original (for SUBMISSION) - printed on 01.07.1999 01:08:25 PM

10-5	International Searching Authority	ISA/EP
10-6	Transmittal of search copy delayed until search fee is paid	

FOR INTERNATIONAL BUREAU USE ONLY

11-1	Date of receipt of the record copy by the International Bureau	
------	--	--

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.